IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA
CASE NO. 1:24-cv-186

MASON VAUGHAN, *individually and on behalf of himself and all others similarly situated*, Plaintiffs, v. DELTA DELTA DELTA FRATERNITY, DELTA DELTA DELTA FOUNDATION, DELTA DELTA DELTA PARK STREET PROPERTIES, LLC, and DELTA DELTA DELTA NATIONAL HOUSE CORPORATION, Defendants.	)	**CLASS ACTION COMPLAINT (JURY TRIAL DEMANDED)**

Plaintiff Mason Vaughan ("Plaintiff"), on behalf of himself and all others similarly situated ("Class Members"), files this Class Action Complaint ("Complaint") against Defendants Delta Delta Delta Fraternity, Delta Delta Delta Foundation, Delta Delta Delta Park Street Properties LLC, and Delta Delta Delta National House Corporation (collectively, "Tri Delta" or "Defendants") and complains and alleges upon personal knowledge as to himself and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Defendants for its failure to safeguard and secure the personally identifiable information ("PII") of more than 400 individuals, including Plaintiff. The affected individuals include former and current employees of Defendants, whose PII was maintained by Defendants, as well as potentially current members and alumnae of Defendants whose PII were maintained by Defendants.

2. The data reportedly exposed in the breach includes some of the most sensitive types of data that cybercriminals seek in order to commit fraud and identity theft, such as Social Security numbers and, for employees, W-2 tax information. As a result of Defendants' negligence, on or about March 5, 2024, allegedly through a "phishing scam," cybercriminals were able to gain access to Defendants' computer records and access this sensitive and valuable PII (the "Data Breach"). According to Defendants, information disclosed in the Data Breach includes, but is not limited to, names, addresses, and Social Security numbers.

3. Armed with the PII accessed in the Data Breach, cybercriminals can commit a variety of crimes including opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, and using Class Members' PII to target other phishing and hacking intrusions.

4. Defendants owed a non-delegable duty to Plaintiff and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure. Defendants breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect putative class members from unauthorized access and disclosure.

5. As a result of Defendants' inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class Members' PII was accessed and disclosed. This action seeks to remedy these failings and the harm caused to Plaintiff and Class Members as a result. Plaintiff brings this action on behalf of himself and all persons whose PII was exposed as a result of the Data Breach.

6. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of financial fraud and identity theft. Plaintiff and Class

Members must now and in the future closely monitor their financial accounts to guard against identity theft.

7. Plaintiff, on behalf of himself and all other Class Members, seeks remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief, including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

8. Plaintiff, on behalf of himself and all other Class Members, asserts claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, and unjust enrichment, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

9. Plaintiff Mason Vaughan is a citizen and resident of Orange County, North Carolina. Plaintiff is a current employee of Defendants. On or around March 5, 2024, Plaintiff received communication from Defendants, notifying him that his PII—specifically all the personal information included on his 2023 W-2 statement—was among the information accessed by cybercriminals in the Data Breach.

10. Had Plaintiff known that Defendants would not adequately protect his and Class Members' PII, he would not have applied to or accepted employment from Defendants and would not have provided his PII to Defendants or any of their affiliates.

11. Defendant Delta Delta Delta Fraternity (the "Fraternity") is a not-for-profit corporation organized and existing under the laws of Illinois. Upon information and belief, the

Fraternity's principal office is located at 14951 North Dallas Parkway, Suite 500 in Dallas, Texas 75254.

12. Defendant Delta Delta Delta Foundation (the "Foundation") is a not-for-profit corporation organized and existing under the laws of Texas, registered to do business in North Carolina. Upon information and belief, the Foundation's principal office is located at 14951 North Dallas Parkway, Suite 500 in Dallas, Texas 75254.

13. Defendant Delta Delta Delta Park Street Properties, LLC ("Park Street") is a limited liability company organized and existing under the laws of Oklahoma, registered to do business in North Carolina. Upon information and belief, the Foundation's principal office is located at 14951 North Dallas Parkway, Suite 500 in Dallas, Texas 75254.

14. Defendant Delta Delta Delta National House Corporation ("NHC") is a not-for-profit corporation organized and existing under the laws of Texas. Upon information and belief, the Foundation's principal office is located at 14951 North Dallas Parkway, Suite 500 in Dallas, Texas 75254.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(a) because the amount in controversy exceeds the sum or value of $75,000 and is between citizens of different States.

16. This Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because: (a) there are 100 or more Class Members; (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship; and (c) the aggregate matter in controversy exceeds $5,000,000, exclusive of interests and costs.

17. This Court has personal jurisdiction over each Defendant because: (a) the Foundation and Park Street are both registered to do business in North Carolina and are both presently engaged in substantial activity within the State; and (b) the Fraternity and NHC are both presently engaged in substantial activity within the State.

18. Each Defendant engaged in the conduct underlying this action in North Carolina, including the collection, storage, and inadequate safeguarding of Plaintiff's and Class Members' PII. Defendants intentionally availed themselves of this jurisdiction by employing individuals in this state and maintaining sensitive PII about individuals in this state that were unlawfully disclosed in the Data Breach.

19. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to Plaintiff's claims occurred within this District and Defendant does business in this District.

FACTUAL ALLEGATIONS

A. DEFENDANTS.

20. Tri Delta was founded in 1916 and has availed itself of this jurisdiction since 1931.[1]

21. Tri Delta is a collegiate sorority and advertises itself as "an assembly of women with shared values."[2]

22. However, "[t]he Tri Delta enterprise consists of three separate, not-for-profit entities:" the Fraternity, the Foundation, and NHC, "supported by [Park Street], a property management and employment organization and wholly-owned subsidiary of the Fraternity."[3]

---

[1] Fran Becque & Caroll Lurding, *Delta Delta Delta*, Almanac of Fraternities and Sororities, Urbana: University of Illinois, last updated Jan. 12, 2024.
[2] Tri Delta, *Our Story: Tri Delta Today*, https://www.tridelta.org/our-story/tri-delta-today.
[3] Tri Delta, *Our Story: Careers*, https://www.tridelta.org/our-story/executive-office/careers.

23. Approximately "400 staff members serve the Tri Delta enterprise," including Plaintiff. There are roughly 60 professional staff members working for Tri Delta "as part of the Executive Office team, while more than 300 employees work for [Park Street] in more than 120 chapter facilities across North America."[4]

24. As a condition of employment with Tri Delta, former and current employees like Plaintiff and Class Members were required to provide sensitive PII.

25. In the regular course of its business, Tri Delta collects, stores, and maintains the PII it receives from its former and current employees.

26. By creating and maintaining massive repositories of PII, Defendant has provided a particularly lucrative target for cybercriminals looking to obtain, misuse, or sell such data.

B. THE DATA BREACH AND NOTICE LETTER.

27. According to the Notice Letter received by Plaintiff and Class Members, Defendants noticed that it experienced a data security incident on or about March 4, 2024 and wrote that "official notification of Tri Delta's data breach is forthcoming."

28. The Notice Letter only informed class members that the data breach came as a result of a "phishing scam."

29. The Notice Letter failed to provide documentation regarding the nature and scope of incident, impact on its computer systems, any ongoing investigation, or plans for restoration, other than indicating it would provide class members with free credit monitoring.

30. The information exposed or acquired as a result of the Data Breach is described by Defendants as a "2023 W2 statement which includes your name, address, and Social

[4] *Id*.

Security number." It is unclear from the Notice Letter whether additional PII was also compromised as a result of the data breach. It is likely that more information was exposed in the Data Breach than described in the notifications provided.

31. Defendants did not disclose crucial information, including, but not limited to, how the cybercriminals were able to exploit vulnerabilities in Defendants' IT security systems; the exact extent of information that was collected by Defendants and exposed in the Data Breach; the remedial steps allegedly taken by Defendants when it allegedly took steps to secure its systems; the identity of the hacking or phishing group responsible for the Data Breach; and any specific measures, if any, Defendants have since taken to determine all data which was disclosed, recover the data, and enhance its security safeguards.

32. Defendants recognizes the long-term risks to Plaintiff and Class Members resulting from the Data Breach, as evidenced by their recommendation in the Notice Letter to "place a free fraud alert on your credit file, or consider a credit freeze."

33. However, Defendants failed to provide sufficient notice that credit freezes have substantial drawbacks, including "delay[ing], interfer[ing] with, or prohibit[ing] the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit." 15 U.S.C. § 1681c-1(i)(5).

34. Instead, Defendants only indicate that ongoing credit monitoring services will be provided without any indication as to the length of time the services will be offered, how the sign-up would work and what class members should do while Defendants' investigation moves forward.

35. Defendants' systems accessed by cybercriminals contained Plaintiff's and Class Members' PII that was accessible, unencrypted, unprotected, and vulnerable to acquisition and/or exfiltration by the unauthorized actor.

36. Plaintiff and Class Members provided their PII to Defendants, either directly or indirectly, with the reasonable expectation and mutual understanding that Defendants would comply with its obligation to keep such information confidential and secure from unauthorized access.

37. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Tri Delta assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

C. TRI DELTA KNEW THAT CRIMINALS TARGET PII.

38. At all relevant times, Tri Delta knew or should have known that Plaintiff's and all other Class Members' PII was a target for malicious actors. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class Members' PII from cyber-attacks that Defendants should have anticipated and guarded against.

39. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches preceding the date of the Data Breach, which has been widely reported in the last few years.

40. In the wake of the significant rise in data breaches, the Federal Trade Commission has also issued an abundance of guidance for companies and institutions that maintain individuals' PII.[5]

41. As a result of the notoriety of cyberattacks on systems like Tri Delata's, several other government entities have also issued warnings to potential targets so that they may be alerted and prepared for a potential attack like the Data Breach.

42. In light of the high-profile data breaches and a wealth of relevant guidance and news reports at Defendants' disposal, Defendants knew or should have known that cybercriminals would target its electronic records and stored PII of its former and current employees.

43. These data breaches have been a consistent problem for the past several years, providing Defendants sufficient time and notice to improve the security of their systems and engage in stronger, more comprehensive cybersecurity practices.

44. PII is a valuable property right,[6] and the value of PII as a commodity is measurable.[7] In fact, "[f]irms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[8] American companies are estimated to have spent over $19 billion

---

[5] *See, e.g., Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N., https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last visited Mar. 5, 2024).

[6] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFO. AND COMMC'N. TECH. 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible[.]").

[7] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

[8] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

on acquiring consumers' personal data in 2018—it is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.[9]

45. As a result of its real value and the recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, Social Security numbers, and other PII directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated, becoming more valuable to thieves and more damaging to victims.

46. Consumers place a high value on the privacy of their PII. Researchers shed light on how much consumers value their data privacy -- and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[10]

47. Given these factors, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

48. Therefore, Tri Delta clearly knew or should have known of the risks of data breaches and thus should have ensured that adequate protections were in place, particularly given the nature of the PII stored in its unprotected files and the amount of PII it maintains.

D. PII THEFT HAS GRAVE AND LASTING CONSEQUENCES FOR VICTIMS.

---

[9] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERT. BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[10] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1.

49. Data breaches are more than just technical violations of their victims' rights. By accessing a victim's personal information, the cybercriminal can ransack the victim's life by, *inter alia*, withdrawing funds from bank accounts, getting new credit cards or loans in the victim's name, locking the victim out of their financial or social media accounts, sending out fraudulent communications masquerading as the victim, filing false tax returns, and destroying their credit score or rating.[11]

50. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank or finance fraud.[12] In addition, using the victim's Social Security number, identity thieves may obtain a job, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[13]

51. Identity theft victims are frequently required to spend many hours and large sums of money repairing the adverse impact on their credit.

52. As the United States Government Accountability Office noted in a June 2007 report on data breaches ("GAO Report"), identity thieves use identifying data such as Social Security

---

[11] *See* Laura Pennington, *Recent Data Breach Trends Mean Your Info Was Likely Stolen Last Year*, TOP CLASS ACTIONS (Jan. 28, 2019), https://topclassactions.com/lawsuit-settlements/privacy/data-breach/875438-recent-data-breach/.

[12] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[13] *See Warning Signs of Identity Theft*, FED. TRADE COMM'N, https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft (last visited Mar. 5, 2024).

numbers to open financial accounts, receive government benefits, and incur charges and credit in a person's name.[14]

53. As the GAO Report states, this type of identity theft is more harmful than any other because it often takes time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely; as well as that victims of this type of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[15]

54. Moreover, there may be a time lag between when PII is stolen and used.[16] According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[17]

55. Such personal information is such a crucial commodity to identity thieves that once the information has been compromised, criminals often trade the information on the black market for years. As a result of recent large-scale data breaches, identity thieves and cybercriminals have openly posted stolen credit card numbers, Social Security numbers, and other PII directly on various websites, making the information publicly available.

---

[14] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOV'T ACCOUNTABILITY OFF. (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[15] *Id*.

[16] For example, on average, it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information. John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9, 12 (2019), https://www.iiisci.org/Journal/PDV/sci/pdfs/IP069LL19.pdf.

[17] U.S. GOV'T ACCOUNTABILITY OFF., *supra* n.36 at 29 (emphasis added).

56. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, whom companies employ to find flaws in their computer systems, stating, "[i]f I have your name and your Social Security number and you haven't gotten a credit freeze yet, [then] you're easy pickings."[18]

57. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft, and some need over a year.[19]

58. Now, Plaintiff and Class Members must vigilantly monitor their financial accounts and their family members' accounts for many years to come.

59. It is within this context that Plaintiff and all Class Members must now live with the knowledge that their PII is forever in cyberspace, taken by people willing to use that information for any number of improper purposes and scams, including making the information available for sale on the black market.

E. DAMAGES SUSTAINED BY PLAINTIFF AND CLASS MEMBERS.

60. Plaintiff and all other Class Members have suffered injury and damages, including but not limited to: (1) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (2)

[18] Patrick Lucas Austin, *'It is Absurd.' Data Breaches Show It's Time to Rethink How We Use Social Security numbers, Experts Say*, TIME (Aug. 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[19] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, Their Families, Friends and Workplaces*, IDENTITY THEFT RES. CTR., https://www.idthecenter.org/identity-theft-aftermath-study/ (last visited Mar. 5, 2024).

improper disclosure of their PII; (3) deprivation of the value of their PII, for which there is a well-established national and international market; (4) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face; and (5) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

61. Plaintiff and Class Members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

62. This action is brought and may be properly maintained as a class action pursuant to Rule 23(b)(2) and (3) of the Federal Rules of Civil Procedure.

63. Plaintiff brings this action on behalf of himself and all members of the following Class of similarly situated persons:

> All persons whose PII was accessed in the Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

64. Plaintiff reserves the right to amend the above definition or to propose other or additional classes in subsequent pleadings and/or motions for class certification.

65. Plaintiff is a member of the Class.

66. Excluded from the Class are Defendants and their other affiliates, parents, subsidiaries, officers, agents, and directors, the judge(s) presiding over this matter, and the clerks of the said judge(s).

67. This action seeks both injunctive relief and damages.

68. Plaintiff and the Class satisfy the requirements for class certification for the following reasons:

69. **Numerosity of the Class.** The members in the Class are so numerous that joinder of all Class Members in a single proceeding would be impracticable. While the exact number of Class Members is unknown at this time, Class Members are readily identifiable in Tri Delta's records, which will be a subject of discovery. Upon information and belief, there are thousands of Members in the Class.

70. **Common Questions of Law and Fact.** There are questions of law and fact common to the Class that predominate over any questions affecting only individual members, including:

a. Whether Defendants' data security systems prior to the Data Breach met the requirements of relevant laws;

b. Whether Defendants' data security systems prior to the Data Breach met industry standards;

c. Whether Defendants owed a duty to Plaintiff and Class Members to safeguard their PII;

d. Whether Defendants breached their duty to Plaintiff and Class Members to safeguard their PII;

e. Whether Defendants failed to provide adequate notice of the Data Breach to Plaintiff and Class Members;

f. Whether Plaintiff's and Class Members' PII was compromised in the Data Breach;

g. Whether Plaintiff and Class Members are entitled to injunctive relief; and

h. Whether Plaintiff and Class Members are entitled to damages as a result of Defendants' conduct.

71. **Typicality.** The claims or defenses of Plaintiff are typical of the claims or defenses of the proposed Class because Plaintiff's claims are based upon the same legal theories and violations of law. Plaintiff and Class Members all had their PII stolen in the Data Breach.

Plaintiff's grievances, like the proposed Class Members' grievances, all arise out of the same business practices and course of conduct by Defendants.

72. **Adequacy of Representation.** Plaintiff will fairly and adequately represent the Class on whose behalf this action is prosecuted. His interests do not conflict with the interests of the Class.

73. Plaintiff and his chosen attorneys, Maginnis Howard (collectively, "Plaintiff's Counsel"), are familiar with the subject matter of the lawsuit and have knowledge of the allegations contained in this Complaint. Plaintiff's Counsel are competent in the relevant areas of the law and have sufficient experience to vigorously represent the Class Members. Finally, Plaintiff's Counsel possess the financial resources necessary to ensure that the litigation will not be hampered by a lack of financial capacity and is willing to absorb the costs of the litigation.

74. **Predominance.** The common issues identified above arising from Defendants' conduct predominate over any issues affecting only individual Class Members. The common issues hinge on Defendants' common course of conduct, giving rise to the legal rights sought to be enforced by Plaintiff on behalf of himself and all other Class Members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

75. **Superiority.** A class action is superior to any other available method for adjudicating this controversy. The proposed class action is the surest way to fairly and expeditiously compensate such a large number of injured persons, to keep the courts from becoming paralyzed by hundreds—if not thousands—of repetitive cases, and to reduce transaction costs so that the injured Class Members can obtain the most compensation

possible. Accordingly, class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which, in any event, might cause inconsistent results.

b. When the liability of Defendants have been adjudicated, the Court will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendants to all Class Members, in terms of money damages due and in terms of equitable relief, can be determined in this single proceeding rather than in multiple, individual proceedings where there will be a risk of inconsistent and varying results.

c. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class Members are forced to bring individual suits, the transactional costs, including those incurred by Defendants, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with the identical fact patterns and the same legal issues. A class action will promote a global resolution and uniformity of relief to the Class Members and as to Defendants.

d. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes former and current employees of Defendants, the legal and factual issues are

narrow and easily defined, and the Class Membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class Members can be identified from Defendants' records, such that direct notice to the Class Members would be appropriate

76. **Injunctive relief.** Defendants have acted or refused to act on grounds generally applicable to the Class as a whole, thereby making appropriate final injunctive or equitable relief on a class-wide basis.

FIRST CAUSE OF ACTION
NEGLIGENCE

77. Plaintiff and Class Members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

78. Plaintiff and Class Members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

79. As a condition of employment by Tri Delta, Plaintiff and Class Members were required to and did in fact provide their PII to Defendants.

80. By collecting and storing their PII and using it for commercial gain, at all relevant times, Tri Delta owed a duty to Plaintiff and all other Class Members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, or control.

81. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with statutory and industry standards and to ensure that all Tri Delta's systems and networks and the personnel responsible for them adequately protected the PII.

82. Defendant knew the risks of collecting and storing Plaintiff's and all other Class Members' PII and the importance of maintaining secure systems, and knew of the many data breaches that targeted companies that store PII in recent years.

83. Given the nature of Tri Delta's business, the sensitivity and value of the PII it maintains, and the resources at its disposal, Tri Delta should have identified the vulnerabilities in its systems and prevented the Data Breach from occurring.

84. Tri Delta breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to them -- including Plaintiff's and Class Members' PII.

85. Plaintiff and Class Members are a well-defined, foreseeable, and probable group including former and current employees that Tri Delta was aware of or should have been aware of and could be injured by inadequate data security measures.

86. Plaintiff and Class Members have no ability to protect their PII that was or remains in Tri Delta's possession.

87. It was reasonably foreseeable to Tri Delta that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class Members' PII to unauthorized individuals.

88. But for Tri Delta's negligent conduct and breach of the above-described duties owed to Plaintiff and Class Members, their PII would not have been compromised.

89. Tri Delta's conduct was grossly negligent and departed from reasonable standards of care, including but not limited to failing to adequately protect Plaintiff's and Class Members' PII and failing to provide them with timely notice that their PII had been compromised.

90. Neither Plaintiff nor Class Members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

91. By failing to provide timely and complete notification of the Data Breach to Plaintiff and Class Members, Tri Delta prevented them from proactively taking steps to secure their PII and mitigate the associated threats.

92. As a result of Tri Delta's above-described wrongful actions, inaction, and lack of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class Members have suffered and will continue to suffer economic damages and other injury and actual harm in the form of, *inter alia*: (1) a substantially increased risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (2) improper disclosure of their PII; (3) breach of the confidentiality of their PII; (4) deprivation of the value of their PII, for which there is a well-established national and international market; (5) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and, if applicable, (6) overpayment for the services that were received without adequate data security.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE

93. Plaintiff and Class Members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

94. Plaintiff and Class Members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

95. Defendants had duties by statute to ensure that all information they collected and stored was secure and that they maintained adequate and commercially reasonable data security practices to ensure the protection of Plaintiff's and Class Members' PII.

96. Defendants' duties arise from, *inter alia*, Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1).

97. In relevant part, the FTCA prohibits "unfair…practices in or affecting commerce," including (as interpreted by the Federal Trade Commission ("FTC")) the unfair act or practice by a business, like Tri Delta, of failing to employ reasonable measures to protect and secure PII.

98. The FTC has published numerous guides for businesses that highlight the importance of implementing reasonable data security practices. For example, in 2016, the FTC updated its publication establishing cybersecurity guidelines for businesses, which makes thorough recommendations, including, but not limited to, for businesses to protect the PII they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[20]

99. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or

[20] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N. (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

practice prohibited by Section 5 of the FTCA. Orders resulting from these actions further clarify the measures businesses, like Defendants, must take to meet their data security obligations and effectively put Defendants on notice of these standards.

100. Tri Delta is also subject to North Carolina's Identity Theft Protection Act (the "NCITPA"), which requires, *inter alia*, "a business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form" must provide notice, without unreasonable delay, to victims of security breaches. N.C.G.S. § 75-65.

101. Defendants violated the FTCA and the NCITPA by failing to use reasonable measures to protect Plaintiff's and all Class Members' PII, not complying with applicable industry standards, and delaying notification to affected individuals. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtain and store, and the foreseeable consequences of a data breach involving PII, including, specifically, the substantial damages that would result to Plaintiff and other Class Members.

102. Tri Delta's violation of these federal and state laws constitutes negligence *per se*.

103. Plaintiff and Class Members are within the class of persons that Section 5 of the FTCA was intended to protect, and the harm occurring as a result of the Data Breach is the type of harm against which Section 5 of the FTCA and the NCITPA were intended to guard against.

104. It was reasonably foreseeable to Tri Delta that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems,

would result in the release, disclosure, and dissemination of Plaintiff's and Class Members' PII to unauthorized individuals.

105. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of Defendants' violations of Section 5 of the FTCA and the NCITPA. Plaintiff and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (1) a substantially increased risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (2) improper disclosure of their PII; (3) breach of the confidentiality of their PII; (4) deprivation of the value of their PII, for which there is a well-established national and international market; (5) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and, if applicable, (6) overpayment for the services that were received without adequate data security.

106. Defendants' violations of the FTCA and the NCITPA constitute negligence *per se* for purposes of establishing the duty and breach elements of Plaintiff's negligence claim. Those statutes were designed to protect a group to which Plaintiff belongs and to prevent the type of harm that resulted from the Data Breach.

107. Defendants owed a duty of care to the Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate security practices.

108. It was foreseeable that Defendants' failure to use reasonable measures to protect PII and to provide timely notice of the Data Breach would result in injury to Plaintiff and other Class

Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and the members of the Class were reasonably foreseeable.

109. It was therefore foreseeable that the failure to adequately safeguard PII would result in one or more of the following injuries to Plaintiff and the members of the proposed Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

THIRD CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY

110. Plaintiff and Class Members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

111. Plaintiff and Class Members provided Tri Delta their PII in confidence, believing that Tri Delta would protect that information. Plaintiff and Class Members would not have provided Tri Delta with this information had they known it would not be adequately protected. Tri Delta's acceptance and storage of Plaintiff's and Class Members' PII created a fiduciary relationship between Tri Delta and Plaintiff and Class Members.

112. In light of this relationship, Tri Delta has a fiduciary duty to act primarily for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship, which includes safeguarding and protecting Plaintiff's and Class Members' PII.

113. Tri Delta has a fiduciary duty to act for the benefit of Plaintiff and class members upon matters within the scope of its relationship with its former and current employees, in particular, to secure their PII.

114. Tri Delta breached its fiduciary duties by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' PII and otherwise failing to safeguard Plaintiff's and Class Members' PII that it collected.

115. Tri Delta breached its fiduciary duties by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

116. As a direct and proximate result of Tri Delta's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer injury, including, *inter alia*: (1) a substantially increased risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (2) improper disclosure of their PII; (3) breach of the confidentiality of their PII; (4) deprivation of the value of their PII, for which there is a well-established national and international market; (5) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and, if applicable, (6) overpayment for the services that were received without adequate data security.

FOURTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT

117. Plaintiff and Class Members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

118. In connection with accepting employment by Tri Delta, Plaintiff and all other Class Members entered into implied contracts with Tri Delta.

119. When Plaintiff and Class Members applied or agreed to employment and provided their PII to Defendants, either directly or indirectly, as a pre-condition and in exchange for employment, they entered into implied contracts with Defendants.

120. Pursuant to these implied contracts, and in exchange for the consideration and PII provided by Plaintiff and Class Members, Defendants agreed and Plaintiff (and Class Members) understood that Defendant would, *inter alia*: (1) consider or provide employment to Plaintiff and Class Members; (2) implement reasonable measures to protect the security and confidentiality of Plaintiff's and Class Members' PII; and (3) protect Plaintiff's and Class Members' PII in compliance with federal and state laws and regulations and industry standards.

121. The protection of PII was a material term of the implied contracts between Plaintiff (and Class Members) and Defendants. As set forth *supra*, Tri Delta recognized its duty to provide adequate data security and ensure the privacy of its former and current employees' PII by providing a privacy policy on its website.

122. Plaintiff and Class Members performed their obligations under the implied contract when they provided Defendants with their PII and engaged in employment by Defendants.

123. Plaintiff and Class Members would not have entrusted their PII to Defendants in the absence of such an implied contract.

124. Had Plaintiff and Class Members known that Tri Delta would not adequately protect its former and current employees' PII, they would not have applied to or accepted employment from Defendants.

125. Tri Delta breached its obligations under its implied contracts with Plaintiff and Class Members in failing to implement and maintain reasonable security measures to protect and

secure their PII and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class Members' PII in a manner that complies with applicable laws, regulations, and industry standards.

126. Tri Delta's breach of obligations of its implied contracts with Plaintiff and Class Members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class Members have suffered from the Data Breach.

127. Plaintiff and all other Class Members suffered by Defendants' breach of implied contracts because, *inter alia*: (1) they face a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (2) their PII was improperly disclosed to unauthorized individuals; (3) the confidentiality of their PII has been breached; (4) they were deprived of the value of their PII, for which there is a well-established national and international market; (5) lost time and money incurred, and future costs required, to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and, if applicable, (6) overpayment for the services that were received without adequate data security.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully request that the Court enter judgment in his favor and against Defendant as follows:

a. Certifying that Class as requested herein, appointing the named Plaintiff as Class representatives and the undersigned counsel as Class Counsel;

b. Requiring that Defendants pay for notifying the members of the Class of the pendency of this suit;

c. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

d. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of himself and the Class, seek appropriate injunctive relief designed to prevent Defendants from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend additional credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

e. Awarding Plaintiff and the Class prejudgment and post-judgment interest to the maximum extent allowable;

f. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable, together with their costs and disbursements of this action; and

g. Awarding Plaintiff and the Class such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

This the 6th day of March, 2024.

MAGINNIS HOWARD

/s/ Karl S. Gwaltney
EDWARD H. MAGINNIS
N.C. State Bar No. 39317
KARL S. GWALTNEY
N.C. State Bar No. 45118
7706 Six Forks Road, Suite 101

Raleigh, North Carolina 27615
Tel: (919) 526.0450
Fax: (919) 882-8763
emaginnis@maginnishoward.com
kgwaltney@maginnishoward.com

Counsel for Plaintiff